PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-144756
(43)Date of publication of application : 25.05.2001

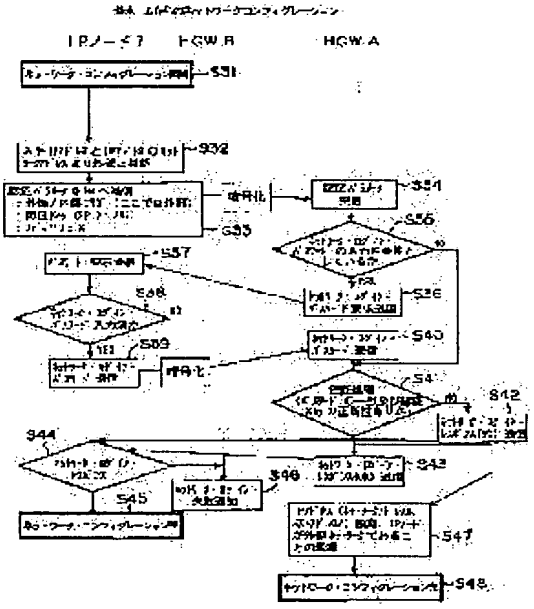
(51)Int.Cl. H04L 12/22
H04L 9/32
H04L 12/46
H04L 12/28
H04L 12/66
H04L 12/56

(21)Application number : 11-327247
(22)Date of filing : 17.11.1999

(71)Applicant : SHARP CORP
(72)Inventor : KIMURA SHINYA
KOBAYASHI YUTAKA

(54) NETWORK CONFIGURATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To network-configurate an optional IP node connected onto an IP network as a desired IP node.
SOLUTION: In this network configuration system of the IP node connected to a network through a public Internet and a gateway GW, the IP node 7 has a means reading authentication information when a card-shaped recording medium on which the authentication information and the address of a home gateway are recorded is inserted, a means (S33) enciphering the read authentication information and transmitting the authentication information to the GW, and means (S44 and S45) network-configurating the IP node when the authentication information transmitted from the GW is decided as proper, and the GW has a means (S41) which collates the transmitted authentication information with information for authentication stored in the GW and decides the identify of the authentication information and means (S42 and S43) transmitting the decision result of the identify of the authentication information to the IP node.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－144756
（P2001－144756A）
(43)公開日　平成13年５月25日(2001.5.25)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*（参考）
Ｈ０４Ｌ　12/22		Ｈ０４Ｌ　11/26		５Ｊ１０４
9/32		9/00	６７３Ａ	５Ｋ０３０
12/46		11/00	３１０Ｃ	５Ｋ０３３
12/28		11/20	Ｂ	
12/66			１０２Ａ	

審査請求　未請求　請求項の数４　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願平11－327247

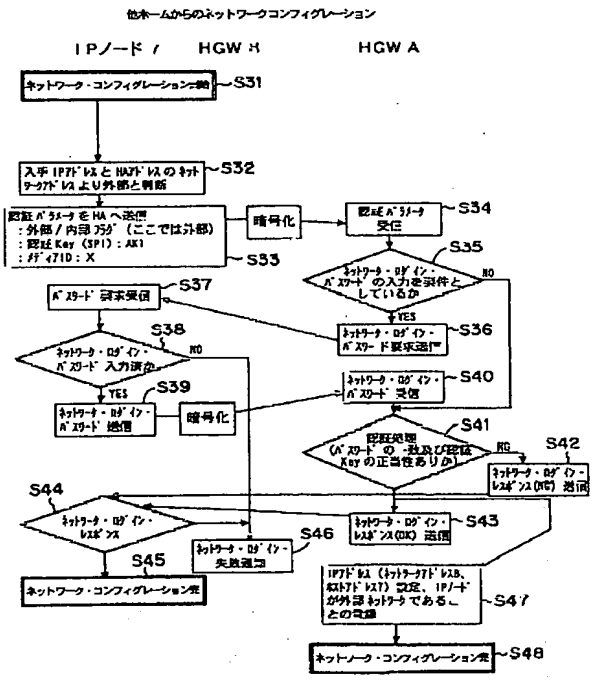
(22)出願日　平成11年11月17日(1999.11.17)

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72)発明者　木村　真也
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(72)発明者　小林　裕
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(74)代理人　100108338
弁理士　七條　耕司　（外１名）

最終頁に続く

(54)【発明の名称】　ネットワーク・コンフィギュレーション方式

(57)【要約】
【課題】　ＩＰネットワーク上に接続される任意のＩＰノードを、所望のＩＰノードとしてネットワーク・コンフィギュレーションする。
【解決手段】　公衆インターネットとゲートウェイＧＷを介しネットワークに接続されるＩＰノードのネットワーク・コンフィギュレーション方式において、前記ＩＰノード７は、認証情報とホームゲートウェイのアドレスを記録したカード状記録媒体が装着時、前記認証情報を読取る手段と、読取った認証情報を暗号化して前記ＧＷに送信する手段（Ｓ３３）と、前記ＧＷから送信された前記認証情報が正当であると判断された時はＩＰノードをネットワーク・コンフィギュレーションする手段（Ｓ４４，Ｓ４５）とを有し、前記ＧＷは、送信された認証情報をＧＷが記憶している認証用情報と照合して認証情報の正当性を判断する手段（Ｓ４１）と、前記ＩＰノードに前記認証情報の正当性の判断結果を送信する手段（Ｓ４２，Ｓ４３）とを有することを特徴とする。



【特許請求の範囲】
【請求項１】　公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークに接続されるＩＰノードのネットワーク・コンフィギュレーション方式において、
前記ＩＰノードは、認証情報とホームゲートウェイのアドレスを記録したカード状記録媒体が装着されたとき前記認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断されたときは当該ＩＰノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報と照合して認証情報の正当性を判断する手段と、前記ＩＰノードに前記認証情報の正当性の判断結果を送信する手段とを有することを特徴とするネットワーク・コンフィギュレーション方式。
【請求項２】　公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークに接続されるＩＰノードのネットワーク・コンフィギュレーション方式において、
前記ＩＰノードは、認証情報とホームゲートウェイのアドレスを記録したカード状記録媒体が装着されたとき前記認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、当該ＩＰノードから入力されたパスワードを前記ホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断され、かつ前記ホームゲートウェイから送信された前記パスワードの一致性の判断結果について一致していると判断されたときは当該ＩＰノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報と照合して認証情報の正当性を判断すると共に、前記送信されたパスワードを当該ホームゲートウェイが記憶している記憶パスワードと対比してパスワードの一致性を判断する手段と、前記ＩＰノードに前記認証情報の正当性の判断結果および前記パスワードの一致性の判断結果を送信する手段とを有することを特徴とするネットワーク・コンフィギュレーション方式。
【請求項３】　公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークと、前記公衆インターネットとゲートウェイを介して相互接続されるネットワークに接続されるＩＰノードのネットワーク・コンフィギュレーション方式において、
前記ＩＰノードは、認証情報とホームゲートウェイのアドレスを記録したカード状記録媒体が装着されたとき前記認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断されたときは当該ＩＰノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報と照合して認証情報の正当性を判断する手段と、前記ＩＰノードに前記認証情報の正当性の判断結果を送信する手段とを有することを特徴とするネットワーク・コンフィギュレーション方式。
【請求項４】　公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークと、前記公衆インターネットとゲートウェイを介して相互接続されるネットワークに接続されるＩＰノードのネットワーク・コンフィギュレーション方式において、
前記ＩＰノードは、認証情報とホームゲートウェイのアドレスを記録したカード状記録媒体が装着されたとき前記認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、当該ＩＰノードから入力されたパスワードを前記ホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断され、かつ前記ホームゲートウェイから送信された前記パスワードの一致性の判断結果について一致していると判断されたときは当該ＩＰノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報と照合して認証情報の正当性を判断すると共に、前記送信されたパスワードを当該ホームゲートウェイが記憶している記憶パスワードと対比してパスワードの一致性を判断する手段と、前記ＩＰノードに前記認証情報の正当性の判断結果および前記パスワードの一致性の判断結果を送信する手段とを有することを特徴とするネットワーク・コンフィギュレーション方式。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＩＰネットワーク上に接続される任意のＩＰノードを、所望のＩＰノードとして容易にコンフィギュレーションすることを可能にしたネットワーク・コンフィギュレーション方式に関する。
【０００２】
【従来の技術】従来、ＬＡＮ等のセキュリティが必要なネットワークに対して、パーソナルコンピュータ（以下、ＰＣという）等をＩＰノードとしてＬＡＮ上にコン

フィギュレーションするためには、ＰＣ毎に何らかのマニュアルによりセットアップ作業が必要であり、また、ＩＰネットワーク上の外部のネットワークに接続したＰＣから前記ＬＡＮにログインする場合には、ＰＣに前記ＬＡＮ上のリモートアクセスサーバと認証手続きをするためのパスワード設定やソフトウエアを実装するとともに、マニュアルによりログインするための入力作業を必要とする。また、モバイルＩＰ（Ｍｏｂｉｌｅ　ＩＰ）のプロトコルで前記ＬＡＮに接続する場合は、モバイルＩＰが前記プロトコルを実装しているとともに、前記ＬＡＮ上のホームエージェント（Ｈｏｍｅ　Ａｇｅｎｔ）等の情報が設定されている必要がある。

【０００３】特開平１１－２５２０６８号公報には、他の通信装置上に自己のデータ通信環境を設定し、遠隔地からでも特定の相手側通信装置に安全かつ最適にアクセスするために、自己のデータ通信を構築するための情報と認証用の情報を記録したＩＣカードを通信装置にセットして本人証とカード認証を行い、通信中継装置において通信装置から取得した情報から相手側通信装置を特定し、その相手側通信装置の公開鍵を用いて電子署名を復号化し、通信装置の通信中継装置に対する正当性を認証し、通信装置、通信中継装置、相手側通信装置間で通信可能とする技術が開示されている。

【０００４】

【発明が解決しようとする課題】しかし、上記のＬＡＮ等のセキュリティにより保護されているネットワークに外部ネットワークからログインするためには、認証を含んだリモートアクセスのためのソフトウェアとログインのためのパスワードやＩＤを設定してあるＰＣ自体を持ち歩くか、また、モバイルＩＰの場合も、モバイルＩＰのプロトコルを有するソフトウェアとホームエージェントへの登録のためのアドレスが設定されているモバイルＩＰを持ち歩かなければならず、その度に、ソフトウェアの設定をする必要があり面倒であった。

【０００５】また、上記公報の技術は、データ通信を構築するための情報と認証用の情報を記録したＩＣカードを通信装置に装着して、通信装置側でデータ通信環境の構築と認証を行うようにして、データ通信のためのユーザの利便性を高めようとするものであるが、ＩＣカード内に認証に係わる情報が多く、また認証処理のために通信装置、通信中継装置、相手側通信装置間での処理を必要としシステムが複雑化する問題がある。

【０００６】本発明の目的は、上記の種々の問題点に鑑みて、カード等の記憶メディアにログインしたいネットワークへのログイン情報を記憶することにより、前記ネットワークまたはＩＰネットワーク上の他のネットワークの任意のＩＰノードに前記記憶メディアを装着することにより、装着されたＩＰノードを自らのネットワーク上のＩＰノードとして利用できるように自動的にコンフィギュレーションすることを可能にしたネットワーク・コンフィギュレーション方式を提供することにある。

【０００７】

【課題を解決するための手段】本発明は、上記の課題を解決するために、次のような手段を採用した。

【０００８】第１の手段は、公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークに接続されるＩＰノードのネットワーク・コンフィギュレーション方式において、前記ＩＰノードは、認証情報とホームゲートウェイのアドレスを記録したカード状記録媒体が装着されたとき前記認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断されたときは当該ＩＰノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報と照合して認証情報の正当性を判断する手段と、前記ＩＰノードに前記認証情報の正当性の判断結果を送信する手段とを有することを特徴とする。

【０００９】第２の手段は、公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークに接続されるＩＰノードのネットワーク・コンフィギュレーション方式において、前記ＩＰノードは、認証情報とホームゲートウェイのアドレスを記録したカード状記録媒体が装着されたとき前記認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、当該ＩＰノードから入力されたパスワードを前記ホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断され、かつ前記ホームゲートウェイから送信された前記パスワードの一致性の判断結果について一致していると判断されたときは当該ＩＰノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報と照合して認証情報の正当性を判断すると共に、前記送信されたパスワードを当該ホームゲートウェイが記憶している記憶パスワードと対比してパスワードの一致性を判断する手段と、前記ＩＰノードに前記認証情報の正当性の判断結果および前記パスワードの一致性の判断結果を送信する手段とを有することを特徴とする。

【００１０】第３の手段は、公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークと、前記公衆インターネットとゲートウェイを介して相互接続されるネットワークに接続されるＩＰノードのネットワーク・コンフィギュレーション方式におい

て、前記ＩＰノードは、認証情報とホームゲートウェイのアドレスを記録したカード状記録媒体が装着されたとき前記認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断されたときは当該ＩＰノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報と照合して認証情報の正当性を判断する手段と、前記ＩＰノードに前記認証情報の正当性の判断結果を送信する手段とを有することを特徴とする。

【００１１】第４の手段は、公衆インターネットとホームゲートウェイを介して相互接続されるホームネットワークと、前記公衆インターネットとゲートウェイを介して相互接続されるネットワークに接続されるＩＰノードのネットワーク・コンフィギュレーション方式において、前記ＩＰノードは、認証情報とホームゲートウェイのアドレスを記録したカード状記録媒体が装着されたとき前記認証情報を読み取る手段と、前記読み取った認証情報を暗号化して前記読み取ったホームゲートウェイのアドレスのホームゲートウェイに送信する手段と、当該ＩＰノードから入力されたパスワードを前記ホームゲートウェイに送信する手段と、前記ホームゲートウェイから送信された前記認証情報の正当性の判断結果について正当であると判断され、かつ前記ホームゲートウェイから送信された前記パスワードの一致性の判断結果について一致していると判断されたときは当該ＩＰノードをネットワーク・コンフィギュレーションする手段とを有し、前記ホームゲートウェイは、前記送信された認証情報の暗号化を復号化し、当該ホームゲートウェイが記憶している認証用情報と照合して認証情報の正当性を判断すると共に、前記送信されたパスワードを当該ホームゲートウェイが記憶している記憶パスワードと対比してパスワードの一致性を判断する手段と、前記ＩＰノードに前記認証情報の正当性の判断結果および前記パスワードの一致性の判断結果を送信する手段とを有することを特徴とする。

【００１２】

【発明の実施の形態】本発明の第１の実施形態を図１乃至図５を用いて説明する。

【００１３】はじめに、本実施形態に係るネットワーク・コンフィギュレーションに先だって、記憶メディアへのログイン情報の入力処理について図１および図２を用いて説明する。

【００１４】図１は、カード状記憶媒体として、購入されて未だログイン情報が書き込まれていない空白状態にあるネットワーク・コンフィギュレーション・メディアを示す図であり、図２は、任意のネットワークに設けられるホームゲートウェイＨＧＷ（Ｈｏｍｅ　Ｇａｔｅｗａｙ）によって、ログイン情報が書き込まれたネットワーク・コンフィギュレーション・メディアを示す図である。

【００１５】これらの図において、ホームゲートウェイＨＧＷは、インターネット等の公衆インターネットとＬＡＮ等で構築されたホームネットワーク間のデータの受け渡し機能を有し、ここでは、ルータ（Ｒｏｕｔｅｒ　Ａ）と、状況に応じて意図を理解して自立的な判断に基づいて各種の処理を行い、ホームネットワークＡでモバイルＩＰ通信をサポートするホームエージェント（Ｈｏｍｅ　Ａｇｅｎｔ）と共に、ネットワーク・コンフィギュレーション・メディア０～３にログイン情報を書き込む装置と書き込むためのネットワーク管理テーブルを備えている。ネットワーク・コンフィギュレーション・メディア０～３は、購入時は、それぞれメディアＩＤ　Ｘ～ＩＤ　Ｗを有しているが、ホームエージェントＨＡのホームアドレスおよび認証キー（ＳＰＩ：Ｓｅｃｕｒｉｔｙ　ｐａｒａｍｅｔｅｒ　Ｉｎｄｅｘ）は空白の状態にある。

【００１６】ネットワーク・コンフィギュレーション・メディア０～３への、ログイン情報の書き込みは、図２に示すように、ネットワーク管理テーブルを有するホームゲートウェイＨＧＷ　Ａに各ネットワーク・コンフィギュレーション・メディア０～３を装着することにより自動的に行われる。先ず、ホームゲートウェイＨＧＷＡに各ネットワーク・コンフィギュレーション・メディア０～３からメディアＩＤ　Ｘ～ＩＤ　Ｗが入力され、それに応じて、各ネットワーク・コンフィギュレーション・メディア０～３に、それぞれホームエージェントＨＡのホームアドレスＡ、認証キー（ＳＰＩ）ＡＫ１～ＡＫ４が付与される。さらに、必要に応じて、ネットワーク・ログイン・パスワードＸＸ～ＺＺを付与するようにしてもよい。ネットワーク・ログイン・パスワードが付与されている場合は、ネットワーク・コンフィギュレーション・メディアの紛失時等において他人の不正使用を防止することができる。

【００１７】次に、ログイン情報が書き込まれたネットワーク・コンフィギュレーション・メディアを用いて、本実施形態に係るホームネットワークにおけるＩＰノードのネットワーク・コンフィギュレーションについて図３乃至図５を用いて説明する。

【００１８】図３は、ＩＰノード０にネットワーク・コンフィギュレーション・メディア０を装着してＩＰノード０をネットワーク・コンフィギュレーションしようとしている状態を示す図であり、図４は、ＩＰノード０のネットワーク・コンフィギュレーションが終了した状態を示す図である。

【００１９】これらの図において、ネットワークＡは、

ルータAおよびホームアドレスAを有するホームエージェントHAからなるホームゲートウェイHGWを介してインターネット網に接続されている。IPノード1～3は、既にホームネットワークAに接続され、ホームゲートウェイHGWのルータAのDHCPサーバからIPアドレスであるA1～A3（ネットワークアドレスA・ホストアドレス0～3）を付与されたノードであり、IPノード0は、例えば、新規に購入される等して、ネットワークAに接続され、IPアドレスの割り当ておよびネットワーク・コンフィギュレーションを行うノードである。ネットワーク・コンフィギュレーション・メディア0は、メディアID　Xを有し、既にホームアドレスA、および認証キー（SPI）AK1のログイン情報が入力されたものである。

【0020】図5は、ホームネットワークAにおいて、ネットワーク・コンフィギュレーション・メディア0を用いてIPノード0をネットワーク・コンフィギュレーションするための処理手順を示すフローチャートである。

【0021】ステップ1において、ホームネットワークAにIPノード0を接続し、ログイン情報が書き込まれたネットワーク・コンフィギュレーション・メディア0をIPノード0に装着することによりネットワーク・コンフィギュレーションが開始される。ステップ2では、ホームエージェントHA　AとIPノード0間でデータリンクレベルでの接続処理が行われ、データリンクが確立する。ステップ3では、ホームゲートウェイHGW AのルータAのDHCPサーバにより、IPノード0に対してIPアドレス（ネットワークアドレスA，ホストアドレス0）を割り当てる。ステップ4では、IPノード0は、入手したIPアドレス（ネットワークアドレスA，ホストアドレス0）とホームエージェントHAのネットワークアドレスAとを対比して、IPノード0がホームネットワークA内部にあることを判断する。ステップ5では、IPノード0は認証パラメータをホームゲートウェイHGWのホームエージェントHA　Aにデータを暗号化して送信する。送信内容は、IPノード0がホームネットワークA内部であることを示すフラグと、ネットワーク・コンフィギュレーション・メディア0から入手した認証キー（SPI）AK1、メディアID　Xである。ステップ6でホームエージェントHA　Aは認証パラメータを受信して、ステップ7で、ネットワーク・ログイン・パスワードが設定されている場合にネットワーク・ログイン・パスワードを必要とするか否かを判断する。ここで、ネットワーク・ログイン・パスワードは、外部フラグが立っているときのみ必要とするようにしてもよいし、また、内部／外部フラグに係わらず必要とするようにしてもよい。ステップ7においてネットワーク・ログイン・パスワードが必要と判断された場合は、ステップ8において、IPノード0に対して、ネットワーク・ログイン・パスワードの送信を要求する。ステップ9でIPノード0がパスワード要求を受信すると、ステップ10で、ネットワーク・ログイン・パスワードの入力を確認し、ネットワーク・ログイン・パスワードが入力されている場合は、ステップ11でホームエージェントHAAにネットワーク・ログイン・パスワードXXを暗号化して送信する。ネットワーク・ログイン・パスワードが入力されていない場合はステップ18においてネットワーク・ログインが失敗であることを知らせる。ステップ12でホームエージェントHA　Aはネットワーク・ログイン・パスワードXXを受信し、ステップ13において、送信されたネットワーク・ログイン・パスワードXXおよび認証キー（SPI）AK1を、図2に示したネットワーク管理テーブルに記憶されているデータと対比して、パスワードの一致性および認証キーの正当性を判断する。一致性および正当性が認められない場合は、ネットワーク・ログイン・レスポンス（NG）をIPノード0に送信し、一致性および正当性が認められた場合は、ネットワーク・ログイン・レスポンス（OK）をIPノード0に送信する。ステップ16において、IPノード0はネットワーク・ログイン・レスポンスを受信し、それがネットワーク・ログイン・レスポンス（OK）の場合は、ステップ17においてIPノード0におけるネットワーク・コンフィギュレーションを完了し、ネットワーク・ログイン・レスポンス（NG）の場合は、ステップ18においてネットワーク・ログインが失敗であることを知らせる。また、ステップ13において、一致性および正当性が認めらた場合は、さらにステップ19において、ホームネットワークA上のIPノード0のIPアドレス（ネットワークアドレスA，ホストアドレス0）を登録すると同時に、ネットワーク・コンフィギュレーション・メディア0が内部ネットワークにあることを登録し、ステップ20でネットワーク・コンフィギュレーションを完了する。

【0022】本実施形態によれば、上記のネットワーク・コンフィギュレーション・メディア0をIPノード0に装着しておくことにより、ネットワーク・コンフィギュレーションされた状態が保持される。ここでネットワーク・コンフィギュレーション・メディア0をIPノード0から外すと、ネットワーク・コンフィギュレーションは解除される。

【0023】なお、本実施形態では、新規に購入しIPノード0をホームネットワークAに接続する場合のコンフィギュレーションについて説明したが、既にネットワーク・コンフィギュレーションされているIPノード0に対して、ネットワーク・コンフィギュレーション・メディア0を装着してネットワーク・コンフィギュレーションしてもよく、その場合はネットワーク・コンフィギュレーション・メディア0に従って、ネットワーク・コンフィギュレーションされ、ネットワーク・コンフィギ

ュレーション・メディア０を外すと元のコンフィギュレーション状態に戻すことができる。

【００２４】このように、本実施形態によれば、ホームネットワークＡにおいて、新規のまたは任意のＩＰノードに対してネットワーク・コンフィギュレーション・メディアを装着することにより、自動的にＩＰノードをネットワーク・コンフィギュレーションすることができる。

【００２５】次に、本発明の第２の実施形態を図６乃至図８を用いて説明する。

【００２６】なお、ネットワーク・コンフィギュレーションに先立つネットワーク・コンフィギュレーション・メディアへのログイン情報の入力処理は第１の実施形態の場合と同じである。

【００２７】図６は、ＩＰノード７にネットワーク・コンフィギュレーション・メディア０を装着してネットワーク・コンフィギュレーションしようとしている状態を示す図であり、図７は、ＩＰノード７に、ネットワーク・コンフィギュレーション・メディア０を装着してネットワーク・コンフィギュレーションが終了した状態を示す図である。

【００２８】次に、ログイン情報が書き込まれたネットワーク・コンフィギュレーション・メディア０を用いて、ホームネットワークＡ外の公衆インターネットに接続された他のネットワークＢに接続されたＩＰノードにおけるネットワーク・コンフィギュレーションについて説明する。

【００２９】図６および図７において、ホームネットワークＡは、図３に示すものと比べてＩＰノード０が接続されていない以外は同じ構成であるので説明を省略する。ネットワークＢは、ルータＢおよびホームアドレスＢを有するホームエージェントＨＡからなるホームゲートウェイＨＧＷ　Ｂを介してインターネット網に接続されている。ここで、ＩＰノード７を含めＩＰノード４～７は、既にネットワークＢに接続され、ホームゲートウェイＨＧＷ　Ｂのルータ Ｂの ＤＨＣＰサーバによりＩＰアドレス（ネットワークアドレスＢ，ホストアドレス４～ネットワークアドレスＢ，ホストアドレス７）を付与されたノードである。ＩＰノード７は、これに操作者が携帯するネットワーク・コンフィギュレーション・メディア０を装着して、ネットワーク・コンフィギュレーションを行おうとするものであり、ネットワーク・コンフィギュレーション・メディア０には、第１の実施形態と同様に、メディアＩＤ　Ｘを有し、既にホームアドレスＡ、および認証キー（ＳＰＩ）ＡＫ１のログイン情報が書き込まれたものである。

【００３０】図８は、ネットワーク・コンフィギュレーション・メディア０を用いて、公衆ネットに接続されるホームネットワークＡ以外の他のネットワークＢに接続されるＩＰノード７をネットワーク・コンフィギュレーションするための処理手順を示すフローチャートである。

【００３１】本実施形態では、ＩＰノード７は、既にネットワークＢに接続されているので、ネットワークＢのホームエージェントＨＡ　ＢからＩＰアドレス（ネットワークアドレスＢ，ホストアドレス７）を付与されている。

【００３２】ステップ３１において、ネットワークＢのＩＰノード７に、ログイン情報が書き込まれたネットワーク・コンフィギュレーション・メディア０を装着することによりネットワーク・コンフィギュレーションが開始される。ステップ３２では、ＩＰノード７は、付与されているＩＰアドレス（ネットワークアドレスＢ，ホストアドレス７）とネットワーク・コンフィギュレーション・メディア０のホームエージェントＨＡ　Ａのネットワークアドレス Ａとを対比して、ＩＰノード７がホームネットワークＡの外部にあることを判断する。ステップ３３では、ＩＰノード７は認証パラメータをホームエージェントＨＡ　Ａにデータを暗号化して送信する。送信内容は、ＩＰノード７がネットワークＡ外部であることを示すフラグと、ネットワーク・コンフィギュレーション・メディア０から入手した認証キー（ＳＰＩ）ＡＫ１、メディアＩＤ　Ｘである。ステップ３４でホームエージェントＨＡ　Ａは認証パラメータを受信して、ステップ３５で、ネットワーク・ログイン・パスワードが設定されている場合に入力することが要件になっているか否かを判断する。ここで、ネットワーク・ログイン・パスワードは、外部フラグが立っているときのみパスワードを必要とするようにしてもよいし、また、内部／外部フラグに係わらずパスワードを必要とするようにしてもよいし、また全く不要としてもよい。ネットワーク・ログイン・パスワードの入力を要件としている場合は、ステップ３６において、ＩＰノード７に対して、ネットワーク・ログイン・パスワードの送信を要求する。ステップ３７でＩＰノード７がパスワード要求を受信すると、ステップ３８で、ネットワーク・ログイン・パスワードの入力を確認し、ネットワーク・ログイン・パスワードが入力されている場合は、ステップ３９でホームエージェントＨＡ　Ａにネットワーク・ログイン・パスワードＸＸを暗号化して送信する。ネットワーク・ログイン・パスワードを入力されていない場合は、ステップ４６においてネットワーク・ログインが失敗であることを知らせる。ステップ４０でホームエージェントＨＡ　Ａはネットワーク・ログイン・パスワードＸＸを受信し、ステップ４１において、送信されたネットワーク・ログイン・パスワードＸＸおよび認証キー（ＳＰＩ）ＡＫ１を、図２に示したネットワーク管理テーブルに記憶されているデータと対比して、パスワードの一致性および認証キーの正当性を判断する。一致性および正当性が認められない場合は、ネットワーク・ログイン・レスポンス（Ｎ

G）をＩＰノード７に送信し、一致性および正当性が認められた場合は、ネットワーク・ログイン・レスポンス（ＯＫ）をＩＰノード７に送信する。ＩＰノード７はネットワーク・ログイン・レスポンスを受信した結果、ステップ４４において、ネットワーク・ログイン・レスポンス（ＯＫ）を受信した場合は、ステップ４５においてＩＰノード７におけるネットワーク・コンフィギュレーションを完了し、ネットワーク・ログイン・レスポンス（ＮＧ）の場合は、ステップ４６においてネットワーク・ログインが失敗であることを知らせる。また、ステップ４１において、一致性および正当性が認められた場合は、さらにステップ４７において、外部ネットワークＢ上のＩＰノード７のＩＰアドレス（ネットワークアドレスＢ，ホストアドレス７）をトネリング先として登録し、同時にネットワーク・コンフィギュレーション・メディア０が外部ネットワークであることを登録し、ステップ４８でネットワーク・コンフィギュレーションを完了する。なお、ここで、ＩＰアドレス（ネットワークアドレスＢ，ホストアドレス７）は、ステップ３３のＩＰアドレス７のホームエージェントＨＡへの認証パラメータの送信時に送信側ＩＰアドレスとして入手することができる。これによって、公衆インターネット上の通信相手からＩＰノード７宛のデータは、ホームエージェントＨＡを経由してトネリングされてネットワークＢ上のＩＰノード７に転送される。

【００３３】上記のごとく、本実施形態によれば、ホームネットワークＡ以外の他のネットワークＢのＩＰノード７にネットワーク・コンフィギュレーション・メディア０を装着することにより、ＩＰノード７をホームネットワークＡ上のＩＰノードと同様に利用できるように自動的にコンフィギュレーションすることができる。また、ネットワーク・コンフィギュレーション・メディア０をＩＰノード７に装着しておくことにより、ネットワーク・コンフィギュレーション状態が確保される。このように、ネットワークＢに接続されているＩＰノード７はあたかもネットワークＡに接続されているかのごとく使用することができ、ホームネットワークＡに自由にアクセスすることができる。ここでネットワーク・コンフィギュレーション・メディア０をＩＰノード７から外すと、先のネットワーク・コンフィギュレーションは解除される。

【００３４】

【発明の効果】本願第１の発明乃至第４の発明によれば、カード状記憶媒体は小型軽量に構成できるので、ユーザはこのカード状記憶媒体を持ち歩くことが可能となり、ユーザは、ＩＰネットワーク上の任意のＩＰノードにこのカード状記憶媒体を装着することにより、ホームネットワークまたはホームネットワーク以外のネットワークに接続されているＩＰノードを自動的にネットワーク・コンフィギュレーションすることができる。

【００３５】また、少なくとも認証情報を記憶した記憶媒体を携帯するだけでよいので、従来技術のように、認証を含んだリモートアクセスのためのソフトウェアやとログインのためのパスワードやＩＤを設定してあるＰＣ自体を持ち歩く必要がなくなる。

【００３６】また、本願第２の発明および第４の発明によれば、ネットワーク・コンフィギュレーションの要件としてパスワードも付加することにより、カード状記憶媒体の紛失時等の不正使用を防止することができる。

【図面の簡単な説明】

【図１】購入されて未だログイン情報が書き込まれていない空白状態にあるネットワーク・コンフィギュレーション・メディアを示す図であり、

【図２】ホームゲートウェイＨＧＷ　Ａによって、ログイン情報が書き込まれたネットワーク・コンフィギュレーション・メディアを示す図である。

【図３】第１の実施形態に係るＩＰノード０にネットワーク・コンフィギュレーション・メディア０を装着してネットワーク・コンフィギュレーションしようとしている状態を示す図である。

【図４】第１の実施形態に係るＩＰノード０におけるネットワーク・コンフィギュレーションが終了した状態を示す図である。

【図５】第１の実施形態に係るホームネットワークＡにおいて、ネットワーク・コンフィギュレーション・メディア０を用いてＩＰノード０をネットワーク・コンフィギュレーションするための処理手順を示すフローチャートである。

【図６】第２の実施形態に係るＩＰノード７にネットワーク・コンフィギュレーション・メディア０を装着してネットワーク・コンフィギュレーションしようとしている状態を示す図である。

【図７】第２の実施形態に係るＩＰノード７におけるネットワーク・コンフィギュレーションが終了した状態を示す図である。

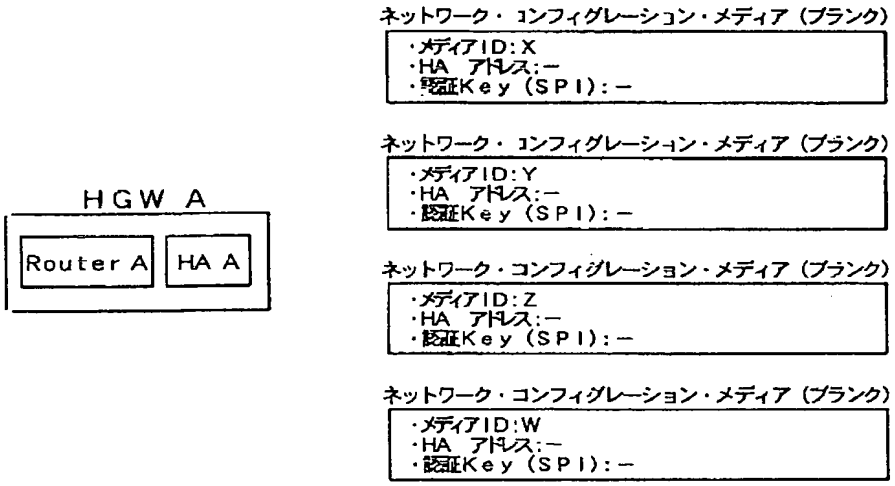
【図８】第２の実施形態に係るネットワーク・コンフィギュレーション・メディア０を用いてホームネットワーク以外の他のネットワークのＩＰノード７をネットワーク・コンフィギュレーションするための処理手順を示すフローチャートである。

【符号の説明】

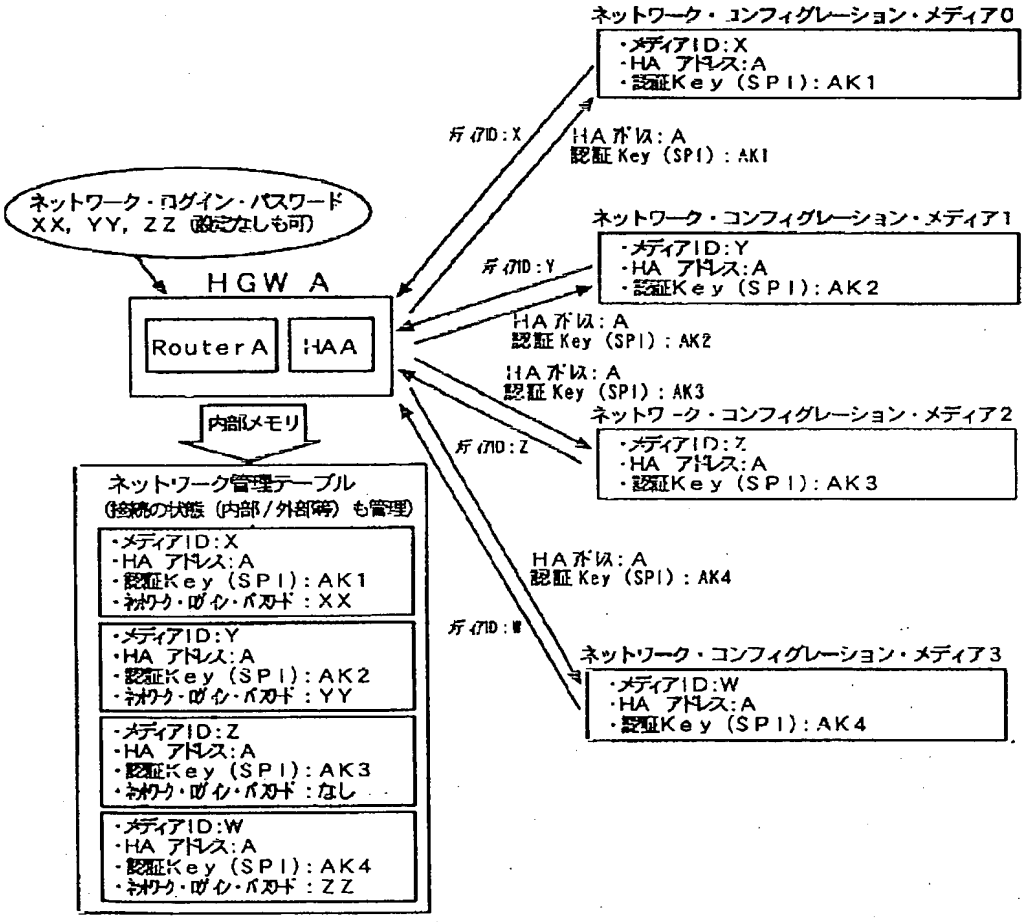
ＨＧＷ　ホームゲートウェイ

ＨＡ　ホームエージェント

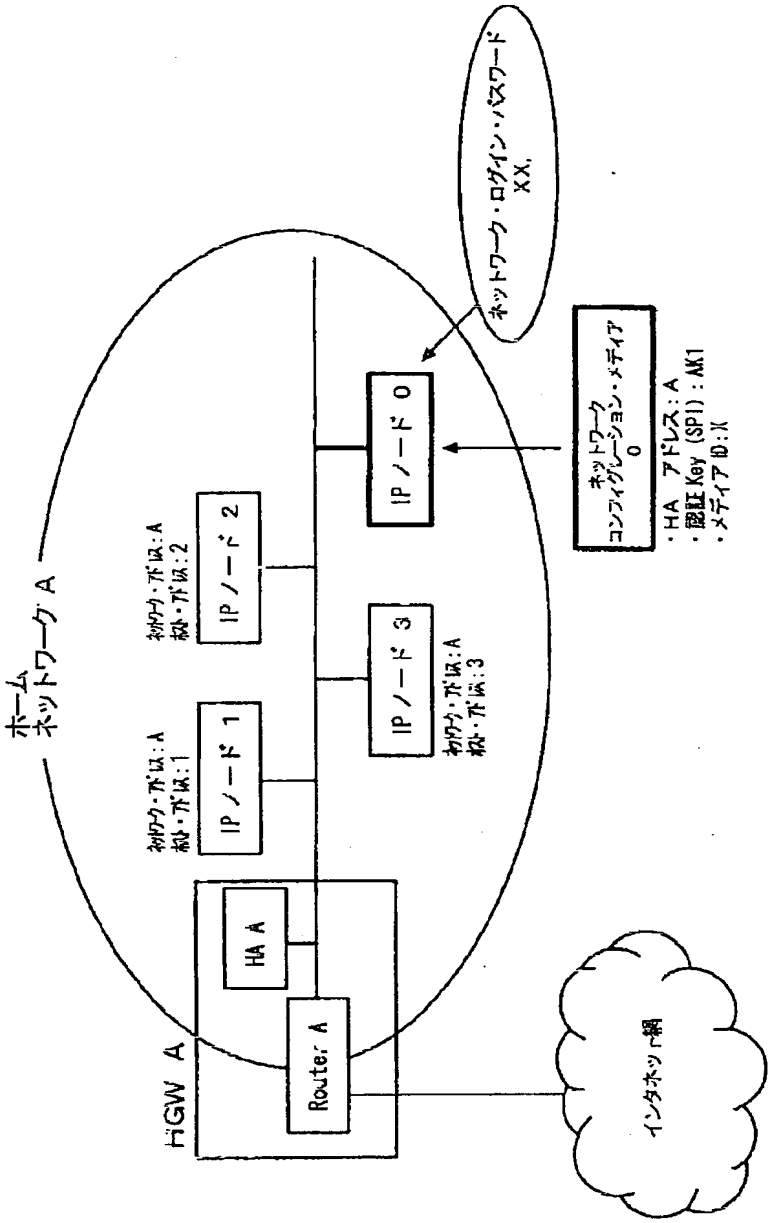
【図1】


HGW A
Router A
HA A
ネットワーク・コンフィグレーション・メディア (ブランク)
・メディアID:X
・HA アドレス:−
・認証Key (SPI):−
ネットワーク・コンフィグレーション・メディア (ブランク)
・メディアID:Y
・HA アドレス:−
・認証Key (SPI):−
ネットワーク・コンフィグレーション・メディア (ブランク)
・メディアID:Z
・HA アドレス:−
・認証Key (SPI):−
ネットワーク・コンフィグレーション・メディア (ブランク)
・メディアID:W
・HA アドレス:−
・認証Key (SPI):−

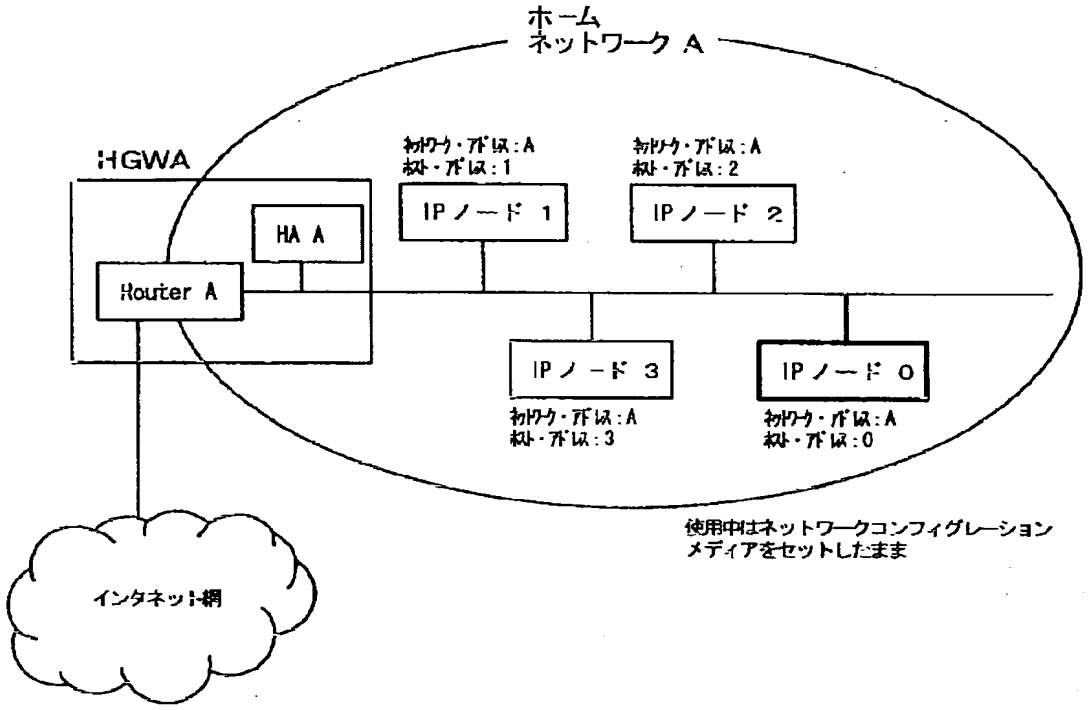
【図2】


ネットワーク・コンフィグレーション・メディア0
・メディアID:X
・HA アドレス:A
・認証Key (SPI):AK1
ネットワーク・コンフィグレーション・メディア1
・メディアID:Y
・HA アドレス:A
・認証Key (SPI):AK2
ネットワーク・コンフィグレーション・メディア2
・メディアID:Z
・HA アドレス:A
・認証Key (SPI):AK3
ネットワーク・コンフィグレーション・メディア3
・メディアID:W
・HA アドレス:A
・認証Key (SPI):AK4
ネットワーク・ログイン・パスワード
XX, YY, ZZ (設定なしも可)
HGW A
Router A
HA A
内部メモリ
ネットワーク管理テーブル
(接続の状態 (内部/外部等) も管理)
・メディアID:X
・HA アドレス:A
・認証Key (SPI):AK1
・ネットワーク・ログイン・パスワード:XX
・メディアID:Y
・HA アドレス:A
・認証Key (SPI):AK2
・ネットワーク・ログイン・パスワード:YY
・メディアID:Z
・HA アドレス:A
・認証Key (SPI):AK3
・ネットワーク・ログイン・パスワード:なし
・メディアID:W
・HA アドレス:A
・認証Key (SPI):AK4
・ネットワーク・ログイン・パスワード:ZZ
HA アドレス:A
認証Key (SPI):AK1
HA アドレス:A
認証Key (SPI):AK2
HA アドレス:A
認証Key (SPI):AK3
HA アドレス:A
認証Key (SPI):AK4

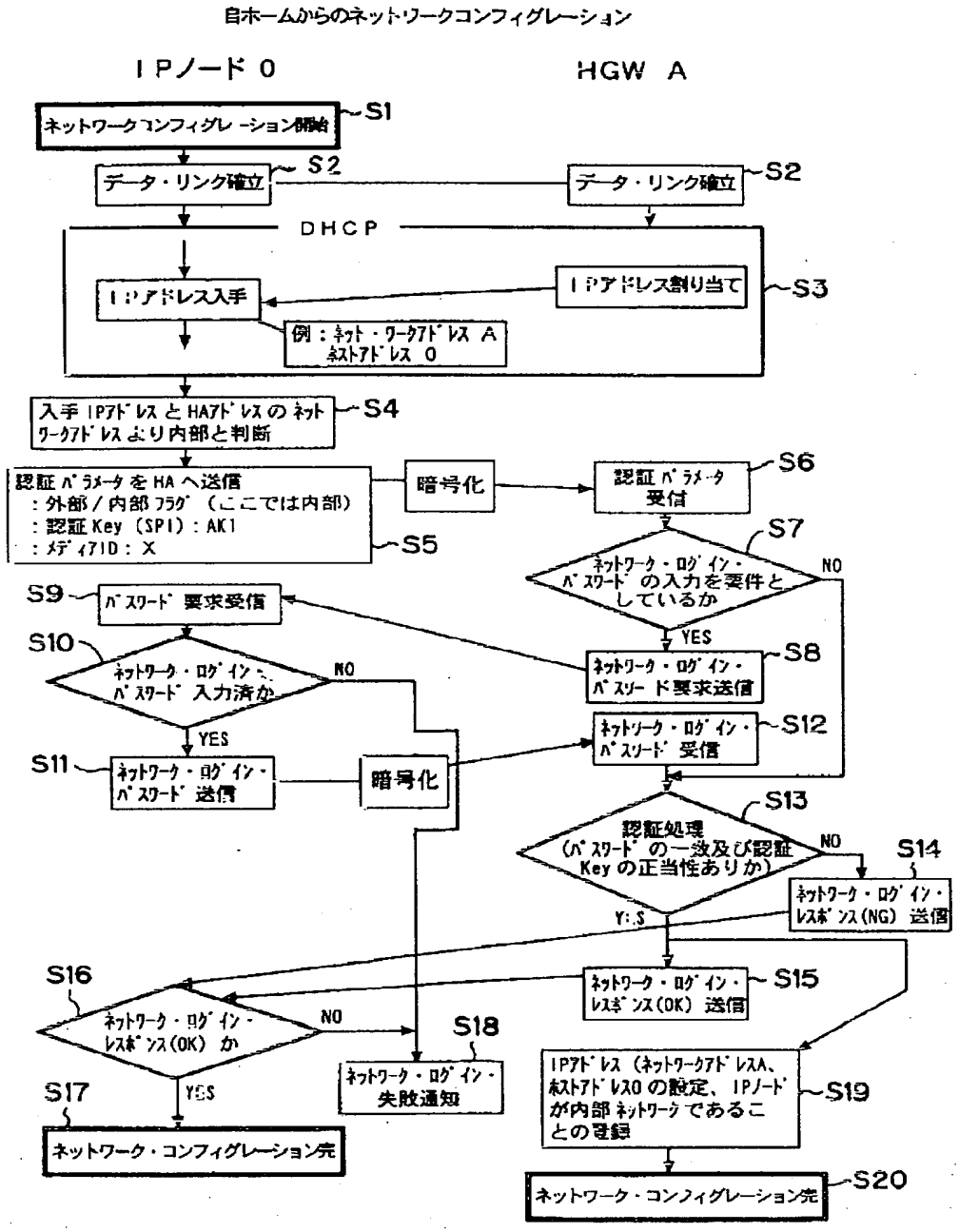
【図3】


ホーム
ネットワーク A
HGW A
Router A
HA A
IP ノード 0
IP ノード 1
IP ノード 2
IP ノード 3
ネットワーク・ロケイン・パスワード
XX,
ネットワーク
コンフィグレーション・メディア
0
・HA アドレス: A
・認証 Key (SPI) : AK1
・メディア ID: K
インタネット網

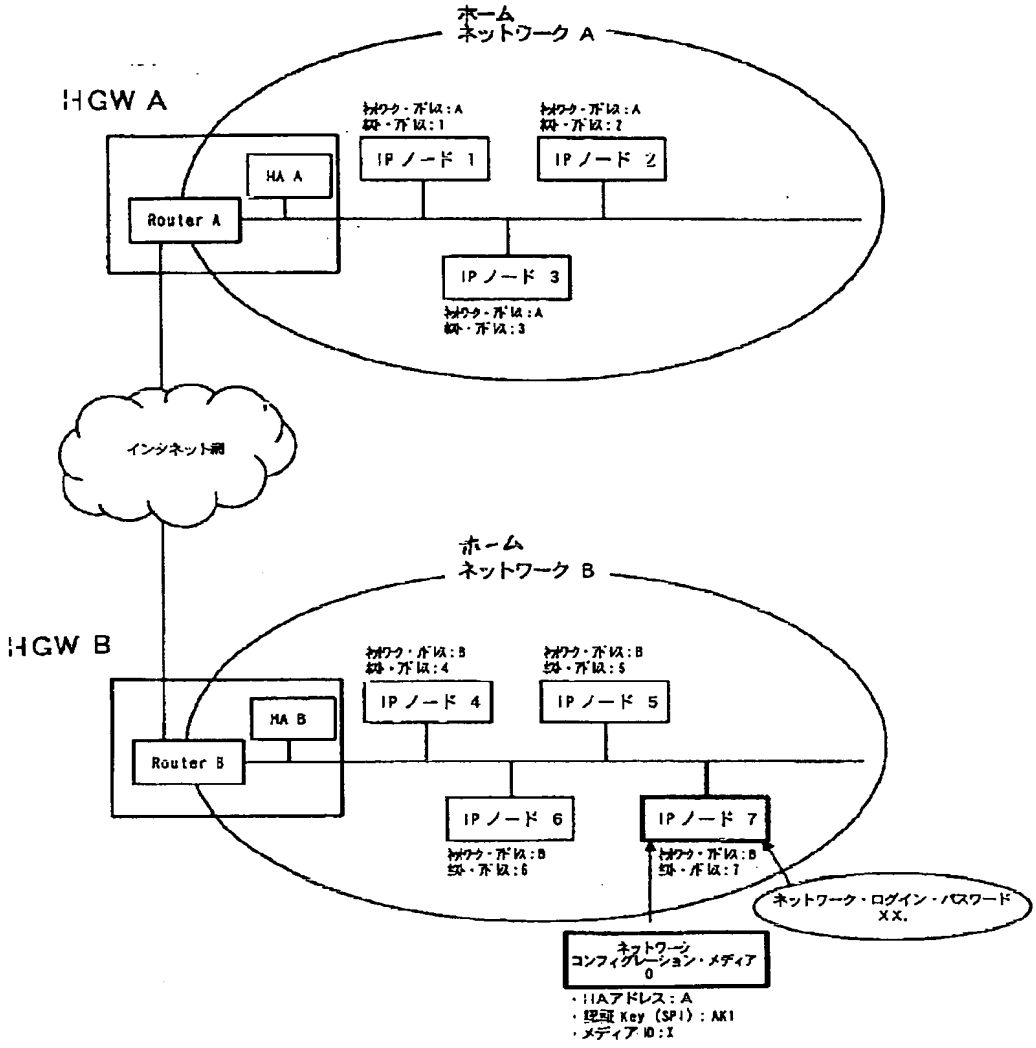
【図4】


ホーム
ネットワーク A
HGWA
HA A
Router A
IP ノード 1
IP ノード 2
IP ノード 3
IP ノード 0
インタネット網
使用中はネットワークコンフィグレーション
メディアをセットしたまま

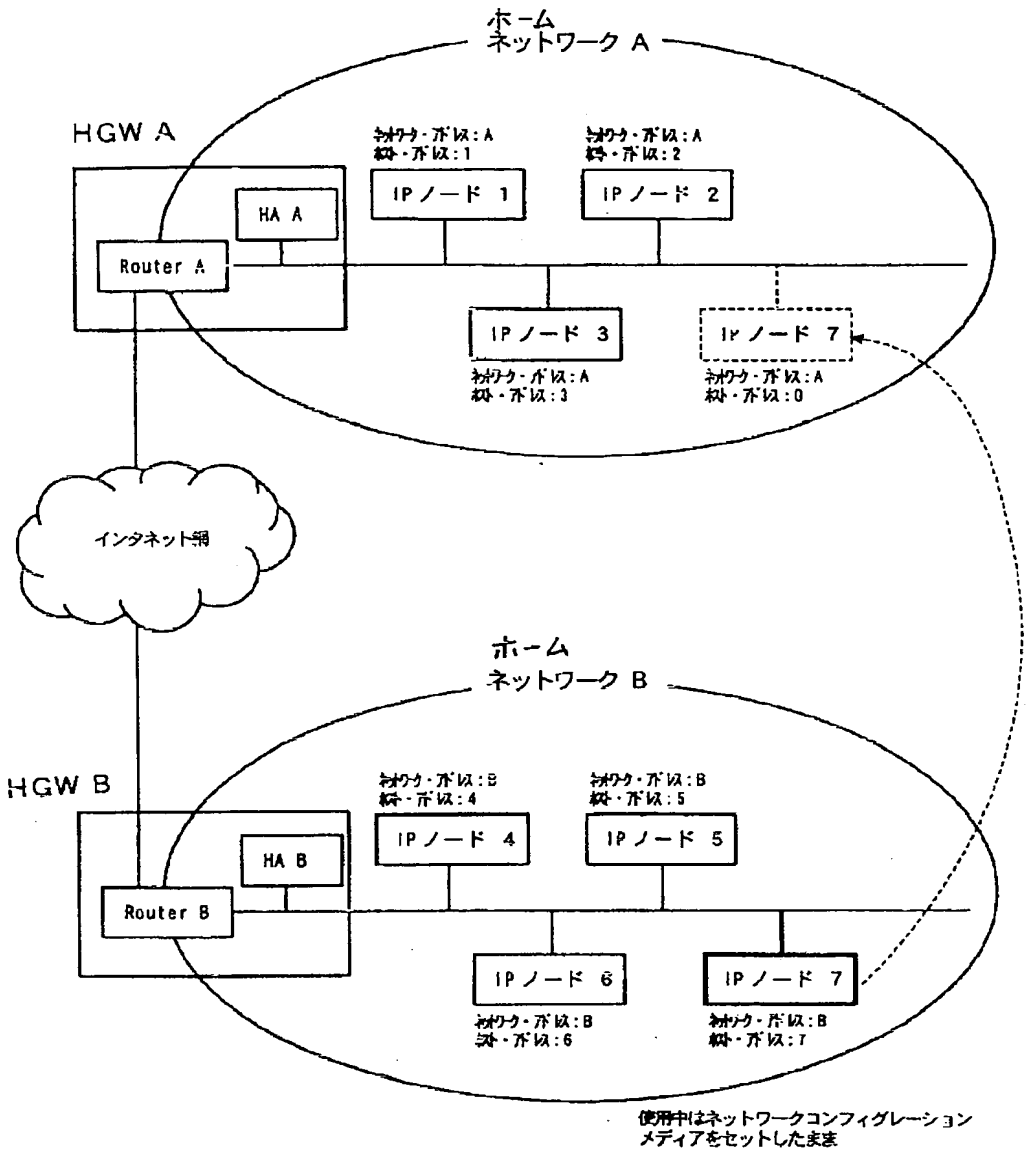
【図5】


自ホームからのネットワークコンフィグレーション
IPノード 0
HGW A
ネットワークコンフィグレーション開始
S1
データ・リンク確立
S2
データ・リンク確立
S2
DHCP
IPアドレス入手
IPアドレス割り当て
S3
例：ネット・ワークアドレス A
ホストアドレス 0
入手 IPアドレス と HAアドレス の ネットワークアドレス より内部と判断
S4
認証パラメータ を HA へ送信
：外部 / 内部 フラグ （ここでは内部）
：認証 Key （SPI）：AK1
：メディアID：X
S5
暗号化
認証パラメータ 受信
S6
ネットワーク・ログイン・パスワード の入力を要件としているか
S7
NO
YES
ネットワーク・ログイン・パスワード 要求送信
S8
S9
パスワード 要求受信
S10
ネットワーク・ログイン・パスワード 入力済か
NO
YES
S11
ネットワーク・ログイン・パスワード 送信
暗号化
ネットワーク・ログイン・パスワード 受信
S12
S13
認証処理（パスワード の一致及び認証 Key の正当性ありか）
NO
S14
ネットワーク・ログイン・レスポンス(NG) 送信
YES
ネットワーク・ログイン・レスポンス(OK) 送信
S15
S16
ネットワーク・ログイン・レスポンス(OK) か
NO
S18
ネットワーク・ログイン・失敗通知
S17
YES
ネットワーク・コンフィグレーション完
IPアドレス（ネットワークアドレスA、ホストアドレスO の設定、IPノード が内部ネットワーク であること の登録
S19
ネットワーク・コンフィグレーション完
S20

【図6】

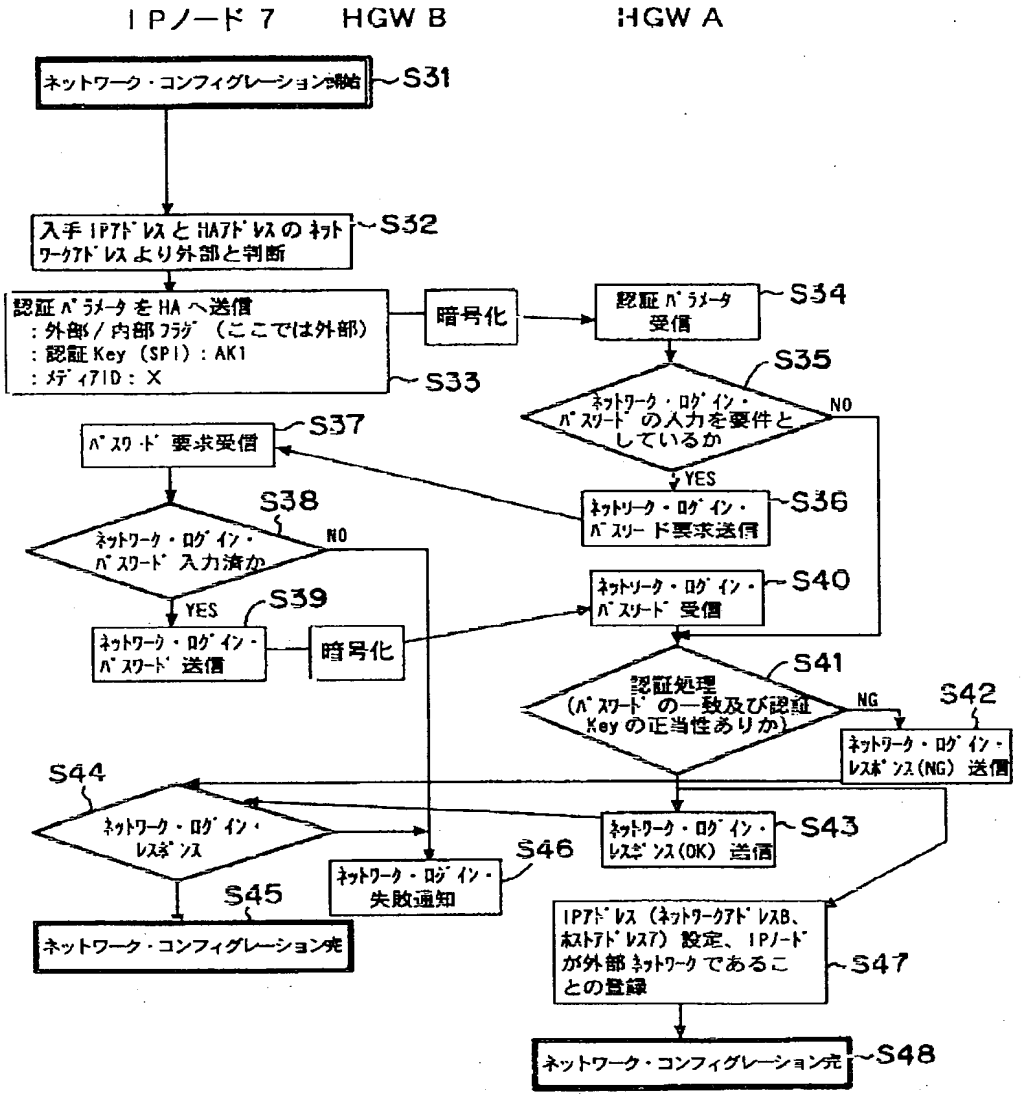

ホーム
ネットワーク A
HGW A
ﾈｯﾄﾜｰｸ・ｱﾄﾞﾚｽ：A
ﾎｽﾄ・ｱﾄﾞﾚｽ：1
ﾈｯﾄﾜｰｸ・ｱﾄﾞﾚｽ：A
ﾎｽﾄ・ｱﾄﾞﾚｽ：2
IP ノード 1
IP ノード 2
HA A
Router A
IP ノード 3
ﾈｯﾄﾜｰｸ・ｱﾄﾞﾚｽ：A
ﾎｽﾄ・ｱﾄﾞﾚｽ：3
インターネット網
ホーム
ネットワーク B
HGW B
ﾈｯﾄﾜｰｸ・ｱﾄﾞﾚｽ：B
ﾎｽﾄ・ｱﾄﾞﾚｽ：4
ﾈｯﾄﾜｰｸ・ｱﾄﾞﾚｽ：B
ﾎｽﾄ・ｱﾄﾞﾚｽ：5
IP ノード 4
IP ノード 5
HA B
Router B
IP ノード 6
ﾈｯﾄﾜｰｸ・ｱﾄﾞﾚｽ：B
ﾎｽﾄ・ｱﾄﾞﾚｽ：6
IP ノード 7
ﾈｯﾄﾜｰｸ・ｱﾄﾞﾚｽ：B
ﾎｽﾄ・ｱﾄﾞﾚｽ：7
ネットワーク・ログイン・パスワード
XX.
ネットワーク
コンフィグレーション・メディア
0
・HAアドレス：A
・認証 Key (SPI)：AK1
・メディア ID：I

【図7】


ホーム
ネットワーク A
HGW A
HA A
Router A
IPノード 1
IPノード 2
IPノード 3
IPノード 7
インタネット網
ホーム
ネットワーク B
HGW B
HA B
Router B
IPノード 4
IPノード 5
IPノード 6
IPノード 7
使用中はネットワークコンフィグレーション
メディアをセットしたまま

【図8】

他ホームからのネットワークコンフィグレーション



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	(参考)
H04L 12/56			

Fターム(参考) 5J104 AA07 KA01 NA05 NA33 NA38
NA41 PA07
5K030 GA10 GA15 GA17 HA08 HC01
HD03 JA10 JT03 KA01 KA06
LA08 LB02 LD19
5K033 AA09 CB01 CB08 CB14 CC01
DA01 DA06 DB20 EA03